--15. A process for the remote authentication of a user (7) for local access to a local machine (4) of a network (5) having a remote server (3) managed by an administrator (8) and classification means (6) for classifying information, and means (9) for connecting the user (7) and the administrator (8) comprising

- creating a challenge (D) capable of being transmitted by the communication means (9);
- communicating the challenge (D) created to the administrator (8) together with elements known by the user, via the communication means (9);
- performing a first predetermined calculation by means of the server (3) and obtaining a first response (RD) that is a function of the challenge (D) and/or of predetermined data;
- transmitting to the user (7) the first response (RD);
- performing a second calculation by means of the local machine (4) and obtaining a second response (RD1) that is a function of the challenge (D) and/or of predetermined data; and
- comparing the first response (RD) transmitted by the administrator to the second response (RD1) calculated by the local machine (4) so as to authenticate the user and locally authorize connection of the user (7) to the local machine (4) based on the result of the comparison.

16. A process according to claim 15, characterized in that the calculation performed by the server (3) consists of modifying, in accordance with a given algorithm, the challenge (D) and/or at least one of the following pieces of data:

a.) at least one piece of information issued by the classification means and known by the user,

b.) at least one secret shared between the server (3) and the local machine (4),

c.) at least one element communicated by the user.

17. A process according to claim 15, characterized in that the calculation performed by the local machine (4) consists of modifying, in accordance with a given algorithm, the challenge (D) and/or at least one of the following pieces of data:

a.) at least one secret shared between the server (3) and the local machine (4),

b.) at least one element communicated by the user.

18. A process according to claim 16, characterized in that the calculation performed by the local machine (4) consists of modifying, in accordance with a given algorithm, the challenge (D) and/or at least one of the following pieces of data:

a.) at least one secret shared between the server (3) and the local machine (4),

b.) at least one element communicated by the user.

19. A process according to claim 16, characterized in that said at least one shared secret is entered into the server (3) and transmitted to the local machine (4) during a successful network authentication.

20. A process according to claim 17, characterized in that said at least one shared secret is entered into the server (3) and transmitted to the local machine (4) during a successful network authentication.

21. A process according to claim 18, characterized in that said at least one shared secret is entered into the server (3) and transmitted to the local machine (4) during a successful network authentication.

22. A process according to claim 16, characterized in that said at least one shared secret or secrets, as the case may be, are modified by means of a modification key (C) that depends on the local machine (4), prior to being modified by the algorithm.

23. A process according to claim 22, characterized in that the modification key (C) consists of concatenating the secret or a combination of secrets existing in the form of a byte string called a Master Station Secret and of hashing the byte string obtained through concatenation by means of a calculation algorithm, to obtain a byte string called a Station Secret.

24. A process according to claim 16, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

25. A process according to claim 17, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

26. A process according to claim 18, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

27. A process according to claim 15, characterized in that the challenge is constituted by a byte string.

28. A process according to claim 16, characterized in that the challenge is constituted by a byte string.

29. A process according to claim 24, characterized in that the challenge is composed of:

- a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;
- second and third bytes representing the version number of the shared information; and
- random alphanumeric characters of the fourth to twelfth bytes.

30. A process according to claim 27, characterized in that the challenge is composed of:

- a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;
- second and third bytes representing the version number of the shared information; and
- random alphanumeric characters of the fourth to twelfth bytes.

24. A process according to claim 16, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

25. A process according to claim 17, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

26. A process according to claim 18, characterized in that said at least one shared secret or secrets, as the case may be, are accompanied by a version number that is incremented each time the secret is modified.

27. A process according to claim 15, characterized in that the challenge is constituted by a byte string.

28. A process according to claim 16, characterized in that the challenge is constituted by a byte string.

29. A process according to claim 24, characterized in that the challenge is composed of:

- a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;
- second and third bytes representing the version number of the shared information; and
- random alphanumeric characters of the fourth to twelfth bytes.

30. A process according to claim 27, characterized in that the challenge is composed of:

- a first byte representing the type of challenge, the type of challenge indicating whether a network authentication has been performed;
- second and third bytes representing the version number of the shared information; and
- random alphanumeric characters of the fourth to twelfth bytes.

31. A process according to claim 23, characterized in that the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string composed of the concatenation in a predetermined order of the challenge, the character string resulting from the transformation by a calculation algorithm of the user's password, the Station Secret and the user's name.

32. A process according to claim 15, characterized in that the response (RD; RD1) is calculated by hashing, in accordance with a calculation algorithm, a character string composed of the concatenation in a predetermined order of the challenge, a fixed security key CC stored in the local machine (4) and in the server (3), the name of the local machine (4), the character string resulting from the transformation by a calculation algorithm of the user's password and user name.

33. A process according to claim 15, characterized in that the local connection authorized is temporary, the authorized duration being configurable.

34. A process according to claim 15, characterized in that it consists of locally authenticating the user (7) after a disconnection by the user (7) authenticated remotely.

35. A system for the remote authentication of a local user (7) for local access to a local machine of a network (5) having a remote server (3) managed by an administrator (8) and containing means (6) for classifying information, comprising communication means (9) for connecting the user (7) with the administrator (8), each local machine (4) comprising a user authentication module (10) that includes a first user module for generating a challenge (11) and a second user module for calculating a response to the challenge, and the remote server (3) comprising an administrative authentication module (13) for authorizing access by the user to the local machine based on the response generated.--.

IN THE ABSTRACT:

Please cancel the Abstract at page 18 and substitute the following new Abstract: